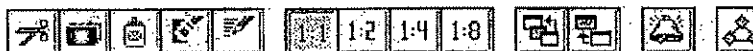


and type. It also shows the security level of the current user and whether the map is in protected (i.e., read-only) mode. See the section *Disabling the Map Editing Feature* in this chapter.



Toolbar OpenView displays a toolbar at the top of the main window.

The toolbar provides quick access to frequently used functions that allow you to create network maps.



CH4-22

The toolbar buttons are described in the following table.

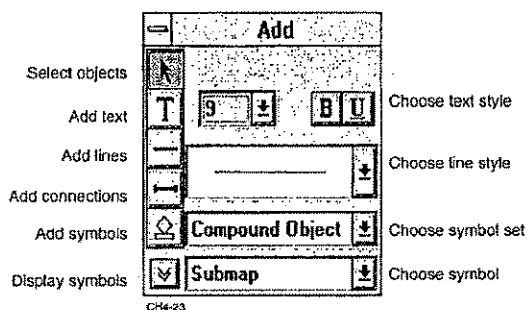
Table 3-2 Toolbar Functions

Tool	Description
Scissors	Cut (same as in the Edit menu).
Camera	Copy (same as in the Edit menu).
Paste	Paste (same as in the Edit menu).
Eraser	Delete (same as in the Edit menu).
Pencil	Describe (same as in the Edit menu).
1:1	Zoom 1 (same as in the View menu).
1:2	Zoom 1/2 (same as in the View menu).
1:4	Zoom 1/4 (same as in the View menu).
1:8	Zoom 1/8 (same as in the View menu).
Home Submap	Display the home submap (same as in the Window menu).
Previous Submap	Display the previous submap (same as in the Window menu).
Alarm Bell	Display the alarm log. Icon color reflects the highest unacknowledged alarm.

Add Toolbox

Choose **Add** from the **Edit** menu to display the toolbox with drawing functions. The **Add Toolbox** contains the following:


- Selection Pointer
- Text
- Lines
- Connections
- Symbols (compound objects, computers, and components)



Click on the appropriate button to select the **Text**, **Lines**, **Connections**, or **Symbols** buttons. Selecting these buttons while holding the **Ctrl** key allows you to make multiple adds of a given symbol without returning to the **Add Toolbox**. Click on the **Select Object** pointer in the **Add Toolbox** to get out of the multiple add mode.

When you draw a map you can display and choose from various styles of text, lines, and symbols.

Applications that run under OpenView can add their own symbols. Refer to your application documentation for additional information. If symbols in the Display symbols list appear as question marks, they are probably symbols added by an application and have not been properly installed. Check for proper installation of applications that use these symbols.

- Select Object** The **Select Object** pointer button is used to restore the cursor to selection mode when in multi-add mode.
- Text** You can select from different combinations of size and style of text. Text is available in 8, 9, 10, 12, and 14 points. You can specify each size using regular, **bold**, or underline styles.
- Lines and Connections** You can select lines in 8 thicknesses. Thin lines are available in five patterns, including solid. If you want the line to be attached ("connected" to a symbol) use the **Connection** button.
- You can use different line types to represent different connections in your network. For example, use a thick line to represent a LAN and a thin line for connections from computers to the LAN.
- Symbol** The **Symbol** button allows you to add selected symbols to a submap. First select a symbol set, **Compound Object**, **Computer**, or **Component**. Then display a list of the available symbols for the set using the list button at the right of the field.
- The **Display Symbols** button can be used to display the icons for a symbol set. When adding a symbol to a submap you can select the symbol from either the text list or the graphic list.
- OpenView provides five **Compound Object** symbols: Submap, GoTo, Personal Computer, Medium Computer, and File Server. OpenView applications may add additional compound icons. A compound object icon can be opened with a double click. In general, symbols for Compound Objects are displayed with a "+" at the end of their names to help differentiate them from Computer and Component symbols.
-  *OpenView stores names entered for compound objects using uppercase characters. OpenView also truncates these names to 15 characters.*
- The Submap symbol (shown as a small network) indicates another submap. The background of the Submap symbol displays the status color of the referenced submap. In a hierarchically structured map, the Submap symbol can be used to point to a lower level submap. Double clicking on the Submap symbol will cause the referenced submap to be displayed.

The GoTo symbol does not display status and can be used to reference any submap. Use the GoTo symbol to link any submaps where you do not want status information to pass between the submaps. Double clicking on the GoTo symbol will cause the referenced submap to be displayed.

Other symbols in the Compound Object category are used for devices that provide internal configuration information to OpenView. If a supporting application is installed, opening one of these could display hardware configuration and status, memory usage, disc space, or installed software.

There are several **Computer** symbols depicting large and medium computers, PCs, and various computer components. OpenView applications can add symbols to or delete symbols from the standard set.

The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols to or delete symbols from the standard set.

Selection Lists

If you frequently make changes to a group of map objects, you can make a list of the objects to use as a group selection function. You can use this list to automatically select the objects to perform operations on them as a group. The effect is the same as if you had selected the objects manually.

Two list commands are available in the **File** menu: **Load Selection List** and **Save Selection List As**. For information about using the Selection List commands, refer to Chapter 4.

Extended Locate

The **Extended Locate** command is in the Window Menu. Extended Locate can be used to find and display the submap containing a particular device or object symbol. It's similar to Locate Object, but with more functionality.

Extended Locate 3-15

Table 3-3 Functions available in **Extended Locate**

Locate By	These buttons allow you to choose the method of finding a device or object. You can search by Object Name, Network Address, Web Site, or MAC Address.
Select on Map	This function selects the desired object on the map.
GoTo	This function displays the submap containing the selected object. If multiple objects are selected from the scroll box window (lower right), then the submap containing the first object in the list is displayed. If multiple objects are selected from the upper left window, then the function will be disabled.
Delete	Deletes the selected object from the map. If multiple objects are selected, then all selected will be deleted from the map. The deleted object(s) remain in the discovery database, and will still be added to the map if another layout is performed.
Options<<	The Options button accesses additional search features.
All Submaps	You can choose the submaps to searches.
All Object Types	You can choose the types of objects on which to perform searches.
Notepad	You can search for notepad entries in object descriptions.
Network Address Types	You can specify which types of network addresses to use in the search.
Miscellaneous search tools	Lines & connections, Unique, Nameless and MacAddr Vendor Names.



3-16

CHAPTER 3: CREATING NETWORK MAPS MANUALLY

4

MONITORING DEVICES ON THE NETWORK

OpenView provides several different ways that you can monitor the devices in your network. You can:

- Customize the access parameters for devices on your network.
- Poll network devices at set intervals to determine the functioning status of each device.
- Monitor trap messages sent by network devices alerting you to changes in device status.
- Configure how alarms are processed, displayed, recorded, and forwarded.

This chapter explains how to configure and use each of these monitoring features.

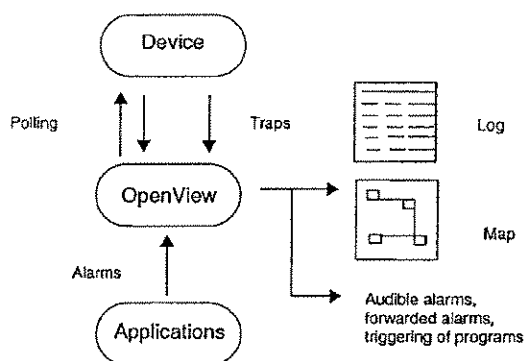
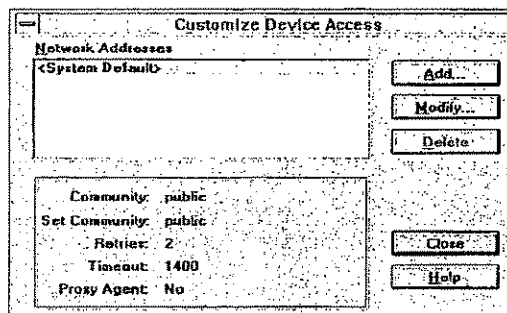


Figure 4-1 Monitoring devices

Customizing Device Access

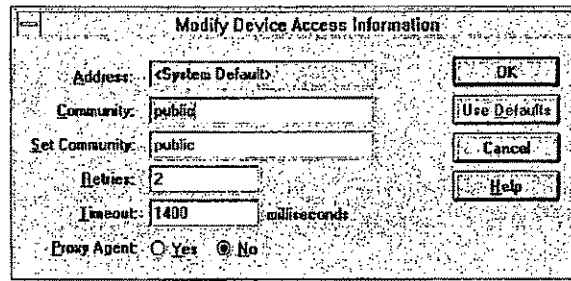
You can associate with a network address control information that is specific to that address. This information is stored in a database that is independent of which map is loaded. For example, you can enter the community name, set community name, and time-out values for devices. These values are used in polling, Autodiscovery, SNMP queries, and third party applications. Devices that you have not customized (devices not in the list) will use the system default values. Only customize the access for devices that require values different from the system default values.

To customize device access, choose **Customize Device Access** from the **Options** menu. The following dialog box appears:



The Customize Device Access dialog box lists the default settings for the selected device's community names, retries and time-out values, and whether it is a proxy agent. A proxy agent is a device that acts on behalf of a device that does not have SNMP capabilities. The trap manager uses the Proxy Agent field.

To change values for any one of the devices listed, select a device and then click on **Modify**. The following dialog box appears:



CHS-02

Type in the new values that you want to change and click **OK**. The values that you entered become the new values for the selected device. Note that the **Community** and **Set Community** passwords are case sensitive.

If you select **Use Defaults** and click **OK**, the entry for this device will be removed from the database because it is no longer an exception and will now use the default system settings.

To change the default values for devices that aren't listed in the Network Addresses list (i.e., the device currently is using system default values), click on **Add**. The Add Device dialog box appears. Type in the network address and then change the values you want. Click **OK**. The address of the device will appear in the Network Addresses list. Note that if you don't change any values, the network address will not appear in the list.

Ping The **Ping** function is used to determine if communication is possible with the selected objects. If the **Ping** is returned, then network communication (TCP/IP or IPX) is functioning correctly for the device. If the **Ping** does not return, it could mean that the network communication for the device is not functioning properly, the device being Pinged is down (or not turned on), or that the device is unreachable from your OpenView console.

The **Ping** command is in the Monitor menu. The **Ping** command can also be accessed with a right-click on any map object. If the object selected does not have a network address configured, an error message is displayed. Objects that normally would not have a network address

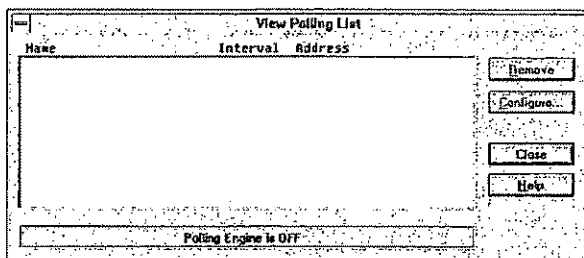
are Submap symbols, Lines, Text, etc. If no object is selected, an error is displayed.

Polling Network Devices

To poll network devices, you perform the following tasks:

- Create a list of the devices that you want to poll
- Set the polling parameters (optional)
- Turn on polling

At any time, you can change the list of devices you want to poll. You can also change the current polling parameters for a specific device using the Configure Device Parameters dialog box. If you do not change the device polling parameters it will use the system defaults. To view the current polling list, choose **View Polling List** from **Polling** in the **Monitor** menu.



CH5-04

A tool bar icon has been added to indicate that polling is active. The symbol in the center of the button rotates when polling is active and is stationary when polling is stopped. You can access the polling menu by clicking on the polling button.

Creating a List of Devices to Poll

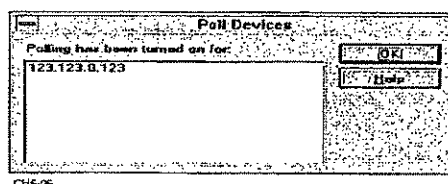
You can poll any device in the map that has an IP or IPX address.

To add a device to poll, follow these steps:

- 1 Select the device(s) on the map that you want to poll.
(Shift-Click or Ctrl-Click can be used to select more than one device.) If you want to poll all of the devices in a submap, select the submap icon.

- 2 Choose Add Device(s) from Polling in the Monitor menu.

The following dialog box appears. The network addresses for the devices that you selected appear in the dialog box.



If a device that you selected to poll has more than one address, a dialog box will ask you to select the address(es) that you want to poll.

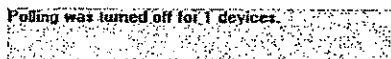
- 3 Click OK.

The list of devices to poll is kept separately with each map. One map with device A may choose to poll the device, another map also showing device A may not poll the device.

Removing Devices to Poll

To remove devices from the polling list, follow these steps:

- 1 Select the devices on the map that you want removed from the polling list.
You can select a single device, multiple devices, or a submap.
- 2 Choose Remove Device(s) from Polling in the Monitor menu.
A message appears telling you how many devices were removed from the polling list.



*You can also remove devices from the polling list using the **Remove** button in the View Polling List dialog box.*

A shortcut for adding and deleting devices in the polling list is to save the selected devices as a Selection List. The list can then be retrieved using Load Selection List. See the discussion of Selection Lists that follows.

Selection Lists

Some applications support operation on a group of objects. If you frequently make changes to a group of map objects, you can make a list of objects to use as a group selection function. You can use this list to automatically select the objects as a group to perform operations on them. The effect is the same as if you had selected the objects manually. Two list commands are available on the **File** menu: **Load Selection List** and **Save Selection List**.



Loading a Selection List

Use the **Load Selection List** command to get a previously saved list. A dialog box will ask for the name of the list file to use. When you enter a file name, the objects listed in the file are automatically selected on your map.

Saving a Selection List

To create a selection list:

- 1 Select a set of symbols and lines with a Shift click on each map object that you want in the list.

Each object that you select must have been described using the **Describe** command.

- 2 Use the Save Selection List As command to save the list to a file.

The default list file name is the current map name with the extension .OVL and is stored in the current map directory. In the future, when you wish to select this set of objects, use the **Load Selection List** command and specify the list file name.

Editing a Selection List

To add or delete objects from an existing selection list:

- 1 Use the Load Selection List command and select the file containing the list that you want to edit.

The objects in the list will be selected on the map.

- 2 To add objects to the list, Shift click the new objects. To delete objects, Shift click on the objects that are already selected.

This will deselect the objects and delete them from the list.

Selection Lists 4-7

- 3 Use the Save Selection List As command to save the list to a file.
All map objects that are selected (highlighted), will be saved in the list.

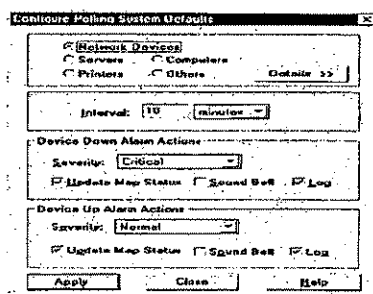
Configuring System Polling Parameters

OpenView has preset default values that control the polling interval and determine what action to take when a device starts or stops functioning. Use system defaults to poll the most devices with the longest interval such as PC's and printers. For large networks you might have to set longer intervals to keep from overloading the system.

To change the system default values, follow these steps:

- 1 Choose Configure System Defaults from Polling in the Monitor menu.

The following dialog box appears.



- 2 Select the desired device class.
- 3 To set the polling interval, enter the appropriate number of hours, minutes, or seconds in the Interval text boxes.
- 4 Select a severity level for the Device Down and Device Up conditions.
- 5 Select what types of action to take for the Device Down and Device Up conditions.

For more information about alarms, see the section, *Configuring Alarms* later in this chapter.

- 6 Click Apply

Configuring Device Types

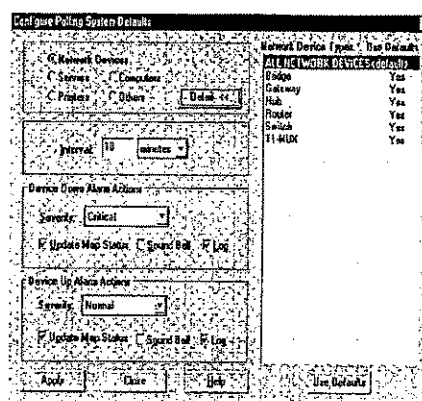
There are system defaults for six classes of device. OpenView uses the same predefined values for each of the device types within the device class. You can modify the default values for each device type in the

class. Use Configuring Parameters for Selected Devices to change the settings for a device at a specific address.

To view the settings for a device class:

- 1 Select a class.
- 2 Click options.

The Configure Polling System Defaults dialog box expands.



CHS-10a.gif

For each class of device there are several device types listed. For example, Network Devices includes bridges, hubs, and routers as device types within the class.

To change the settings for a device type:

- 1 Select a device class.
- 2 Click Options.
- 3 Select the device type.
- 4 Configure interval, etc.

The Use Defaults field for the changed device type will no longer be set to Yes. The default values for each device type in the class can be modified. If a device type does not use the default settings for the class, selecting the device type will display the custom settings.

To restore class default settings to a device type:

- 1 Select the device type.
- 2 Click on Use Defaults.

You can change the overall default settings for the entire class by selecting All Network Devices and then entering values for the polling Interval and Alarm actions.

Configuring Parameters for Selected Devices

You can override the system polling parameters for individual addresses. Use this for setting poll rates for those devices requiring shorter intervals such as routers, bridges, and hubs. Use longer intervals for remote devices.

To do this, follow these steps:

- 1 Select the desired device on the map and choose Configure Device Parameters from Polling in the Monitor menu.

The following dialog box appears.

The screenshot shows a 'Configure Device Parameters' dialog box. It contains the following fields and controls:

- Name:** A text field containing 'LoB #23'.
- Address:** A text field containing '123.123.0.123'.
- Interval:** A spin box set to '5'.
- Severity:** A dropdown menu set to 'Critical'.
- Device Down Alarm Action:** A section with checkboxes for 'Update Map Status' (checked), 'Sound Bell' (unchecked), and 'Log' (unchecked).
- Device Up Alarm Action:** A section with checkboxes for 'Update Map Status' (checked), 'Sound Bell' (unchecked), and 'Log' (unchecked).
- Buttons:** 'Save', 'Use Defaults', 'Close', and 'Help'.

CH5-12

- 2 If you did not select a device on the map, enter the device address that you want to exempt from the system polling values.
Note that you don't have to enter the name.
- 3 Change the values that you want for the polling interval timing, severity, or alarm action.
- 4 Click Save to save the new values. Click Use Defaults to restore the system default values.

4-10

CHAPTER 4: MONITORING DEVICES ON THE NETWORK

Turning Polling On and Off

To start the polling process, choose **Start Polling** from **Polling** in the **Monitor** menu.

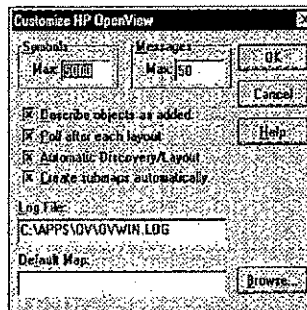
To stop the polling process, choose **Stop Polling** from **Polling** in the **Monitor** menu.

AutoPolling

When OpenView starts, it will automatically discover the devices in your network. It will then create a map of the discovered devices. All devices in the map are automatically added to the polling list. The devices in the polling list will then be polled based on the default polling settings.

To configure automatic polling of discovered devices, choose **Customize HP OpenView** from the **Options** Menu.

The following dialog box appears.



To turn automatic polling **ON**, select **Poll after each layout**.

To turn automatic polling **OFF**, deselect **Poll after each layout**.

Monitoring Traps from Network Devices

Traps are specific types of messages that are generated by some devices to indicate a change in their status. When a device is installed on the network part of its installation procedure is to enter the address of a management console where these traps are to be sent. Refer to the device installation and configuration documentation and set the trap address to the network address of the OpenView console.

OpenView automatically logs an informational alarm for each trap it receives. You can change OpenView's default response to traps to sound an alarm, change color of the map symbol for the device sending the trap, or enter the trap in the alarm log. You can also change the default response to ignore traps from some or all devices, or configure one trap to auto-acknowledge another one when it is received.

Each device class (hub type 1, hub type 2, router, server, etc.) can be assigned a different set of default and customized trap responses. Initially the default trap response for each device class is set to the OpenView system default response. You can change the default response for each device class. In addition, for each device class you can create a customized response for any trap that might be received from a device in that class.

Customizing Traps

Customizing traps consists of:

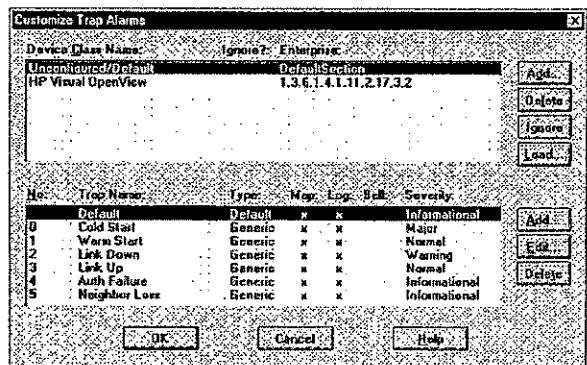
- Selecting the device classes for which you want to customize trap alarm actions
- Selecting or entering the trap IDs for the traps you want to configure
- Choosing what alarm actions to take when OpenView receives the trap

Some device vendors supply trap definition files (.TDF) that can be used to automate trap configuration. If trap definition files have been installed, you can load the predefined traps using the **Load Traps** button. When a device class has been selected, any predefined traps for this device class will be displayed in the **Customized Traps** list.

To customize trap alarms, you use the Customize Traps dialog box. Choose

Customize Traps in the **Monitor** menu. The following dialog box appears.

4-12 CHAPTER 4: MONITORING DEVICES ON THE NETWORK



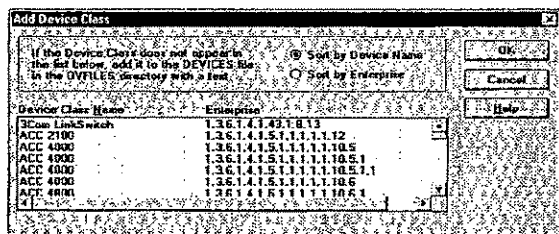
CH5-14

Selecting a Device Class

To select a device class to change the default trap response, follow these steps:

- 1 Click ADD.

The following dialog box appears:



CH5-17

- 2 Select the device class and click OK.

The class name and Enterprise (ObjectID) appears in the Device Class Name list.



To remove a device class from the list, select the device class and click **Delete**.

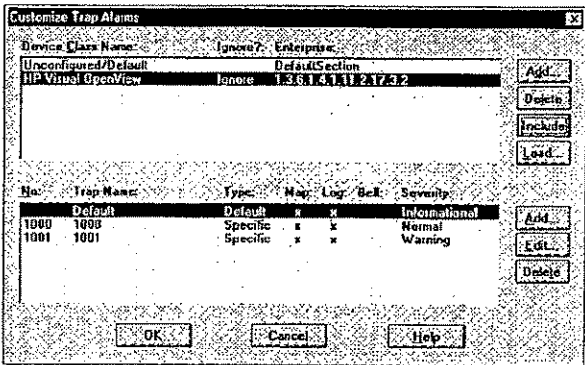
Ignoring Traps

By default, all traps are logged according to the actions configured for the system. If you have another application managing traps for a

particular class of device, you may want OpenView to ignore traps it receives and let the application maintain the device status.

To ignore incoming traps, select the device class whose traps are to be ignored and click **Ignore**. "Ignore" appears in the Flag column next to the device class name.

To turn off Ignore, click **Include**.



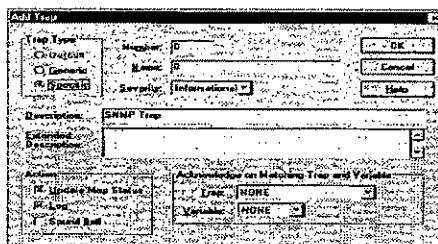
CHS-19

Specifying Traps for a Device Class

You can create a list of the traps that OpenView will respond to for a specific device class. The list of traps will be displayed in the **Customized Traps** list box of the **Customize Traps** dialog box. For a list of traps for a particular device see the manufacturer's documentation.

To add a trap for a device class:

- 1 Click Add. The following dialog box appears:



CH-22

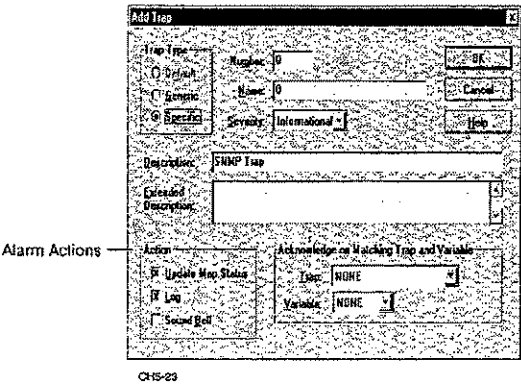
- 2 Select a trap type.
- 3 Type the name (Generic) or the number (Specific) of the trap in the appropriate field.
- 4 Select the desired Alarm Action and Severity.
- 5 Type in a Description.
- 6 Set desired Automatic Acknowledge Alarms.
- 7 Click OK.

The type of trap you selected or entered appears in the Customized Traps list in the Customize Trap Alarms dialog box.

Choosing Trap Alarm Actions

You can choose to update the map status (change color of map symbols), sound a bell, or log an alarm entry when a trap is received. To select any of these options, click on the appropriate Alarm Actions check box(es). To set the severity level you want for the alarm, select the option you want from the Severity list. For the description and extended description fields, you can specify information from the trap packet to be displayed in the Alarm Log.

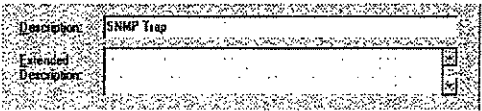
- To select the OpenView response to a trap in the Add Trap dialog box:



- 1 Choose the Severity of the named trap.
- 2 Choose the desired alarm actions (Update map, Sound Bell, Log, etc.).
- 3 Type in a Description.
- 4 Set desired Automatic Acknowledge Alarms.
- 5 Click OK.

**Description Field
Variable Substitution
Syntax**

You can specify how information from the trap packet is displayed in the Description and Extended Description fields using field variables. The extended description allows you to add additional information to the alarm message. The descriptions are entered in the Add Traps dialog box in the following section.



The following table lists the field variables and descriptions.

Table 4-1 Field Variable Table

Variables	Descriptions
\n	newline
\t	tab
\$C	trap community string
\$E	enterprise, represented as a text string if possible
\$e	enterprise, represented as an object ID string of numbers
\$A	name of device that sent the trap. If this device is not represented by a symbol in the map, this field defaults to "addressed" concatenated with the device address.
\$G	generic trap id number
\$S	specific trap id number
\$T	timestamp (time since device was last restarted)
\$*	print all variables in the trap
\$#	number of variables in the trap
\$	print the \$ character
\$n	print the value of the nth variable in the trap, where n is the variable sequence number starting at 1 used to reference subobjects in a device.
\$-n	print the nth variable as a "name-type:value" string, where n is the variable sequence number starting at 1 used to reference subobjects in a device.
\$(+n	print the nth variable as a "name:value" string, where n is the variable sequence number starting at 1 used to reference subobjects in a device.

Loading Traps

You can select a trap definition file (.TDF) from which you can select a device class. In the Customize Trap Alarms dialog box click the **Load** button. Select the desired trap definition file and click **OK**. The traps and their alarm actions for the selected devices class are copied to the trap database (trapmgr.ini).

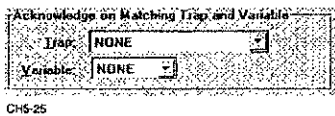
**Automatically
Acknowledging
Alarms Generated
by Traps**

The Acknowledge on Matching Trap and Variable text box allows you to clear a trap when a new specified trap is received. The original trap is moved from the current alarm log to the history alarm log. A variable in the trap packed that holds the network object's name can be selected to match the subobject field in the alarm log. This is to make sure that a trap that clears an alarm is referring to a particular device.

If the device uses a variable in the trap message to more exactly specify which device subcomponent is sending the trap, you can require the

value of this variable to match in the original and acknowledging traps. The variable is used to match the value in the subobject field of the trap message. For example if the trap is from a hub with 16 ports, the trap may contain a value in the subobject field to specify which port caused the trap. Using the variable in the acknowledging trap specification will ensure that if port 7 creates a trap by going down, it will only be cleared by a trap from port 7 going up. This setting will be displayed in the subobject field in the alarm log.

If the subobject field is not used, set it to NONE. Otherwise, set it to the ordinal value of the field (i.e. 1 for the first variable in the trap packet, 2 for the second, etc.).



Managing Alarms

Alarms generated by applications, traps, or polling are managed through the map, alarm log, and alarm forwarding functions.

Selecting Map Status Options

The map symbol of a device is displayed in the color that represents the device status.

To display the available status colors, choose **Status Legend** from the **Monitor menu**. The table below lists the status levels and their colors.

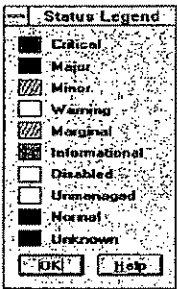


Table 4-2 Map Status Colors Legend

4-18 CHAPTER 4: MONITORING DEVICES ON THE NETWORK

State	Map	Alarm Log	Description
Critical	Red	Red	The device is unavailable. It may be down or in a critical state.
Major	Dark Red	Red	There is a problem with the device. Some degradation of function exists.
Minor	Orange	Yellow	A non critical condition has been reported, or the device is in a degraded state.
Warning	Yellow	Yellow	There is a problem with the device. No degradation of function exists.
Marginal	Mustard	Yellow	The device is approaching shutdown or malfunction.
Informational	Magenta	Magenta	An informational message about this device has been sent by an application.
Disabled	Cyan	Cyan	The device is down.
Unmanaged	Wheat	White	The device is not managed by an OpenView application.
Normal	Green	Green	The device is up and working properly.
Unknown	Blue	Cyan	OpenView has no information on the device's state.



The colors displayed in the alarm log are slightly different than those used on maps.

Status Propagation

You can select the way device status is propagated to higher submap levels using **Customize Alarms** in the **Options** menu. Status propagation can be set to:

- Do not pass status up
- Pass status up one level
- Pass status up all levels

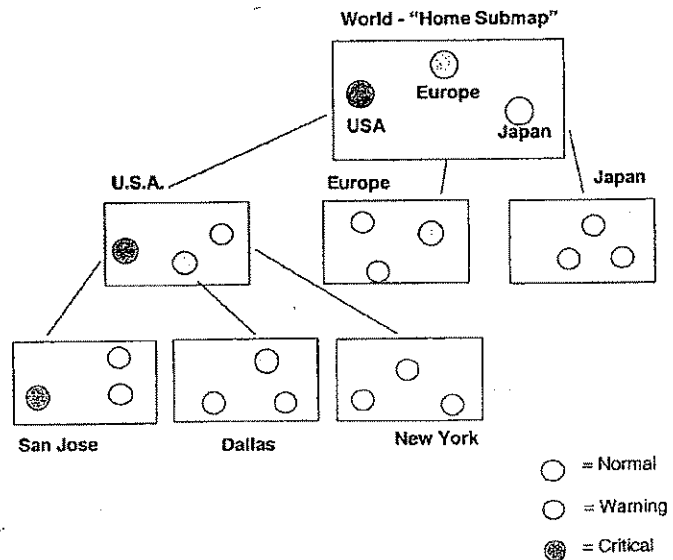
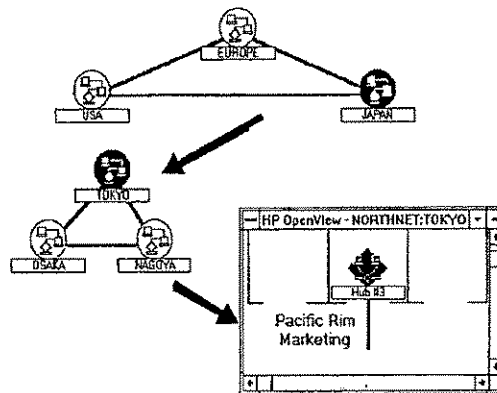


Figure 4-2 Map set to propagate alarms up all levels

Normally, you would select to propagate up all levels. Then, if your home submap contains a submap symbol for each submap in the next lower level in the map, you can check your network's overall status from the home submap. If a submap represents several devices, its submap symbol on the home submap will display the most severe device status for the lower submap. (Note that the GoTo submap symbol does not propagate status.)

You can examine alarms using two methods:

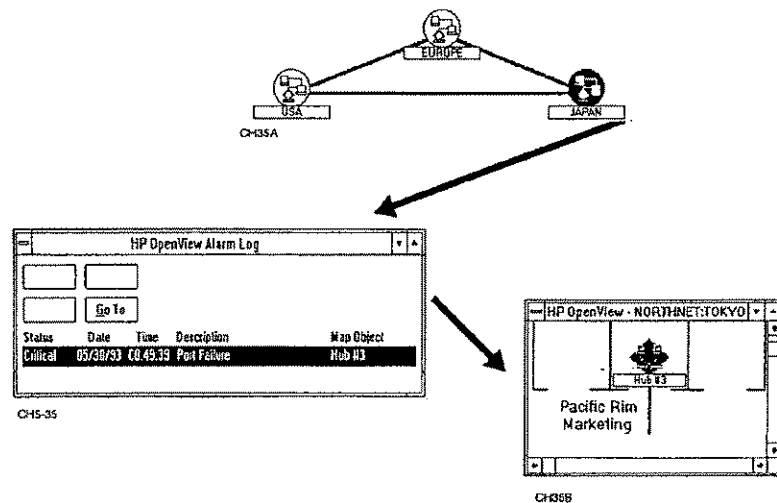
- Using the map, click on the submap symbol showing an alarm status and "walk" down the submap levels until you display the submap containing the device that generated the alarm



CI-15-04

Figure 4-3 Submap containing the device that generated the alarm

- Click **Alarm** in the tool bar or choose **Alarm Log** from the **Monitor** menu to display the **Alarm Log**. Select the alarm that you want to check and then click **GoTo** to display the submap containing the device that generated the alarm.
- Click on the map object using the right mouse button to display the submap containing the device that generated the alarm.
- Click **Alarm** in the tool bar or choose **Alarm Log** from the **Monitor** menu to display the **Alarm Log**. Select the alarm that you want to check and then click **GoTo** to display the submap containing the device that generated the alarm.



- Click on the map object using the right mouse button to display the submap containing the device that generated the alarm.

Configuring Alarms

Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following:

- Change the device symbol to the new status color
- Make an entry in the alarm log
- Forward an alarm to another management console
- Sound an alarm
- Run a program

Regardless of whether OpenView is an active window or not, if a device symbol changes color to red, yellow, or magenta, the Alarm icon in the tool bar changes color and displays the most severe unacknowledged alarm in the log. Alarms of all levels are recorded in the Alarm Log.

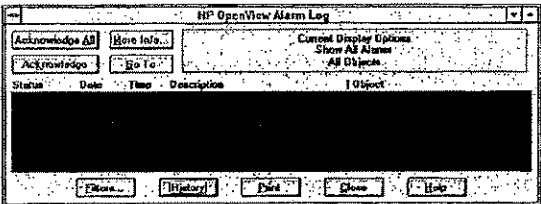


Not all applications monitor device status. Check your device and application documentation to find if a particular network device indicates its status.

Viewing Alarms

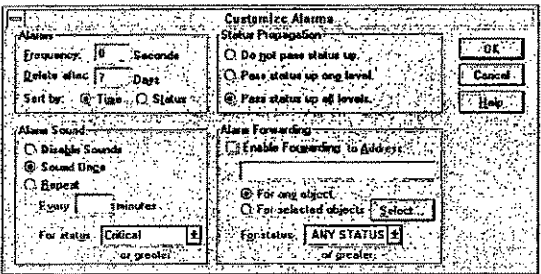
To display the Alarm Log, click on the **Alarm** button in the toolbar or choose **Alarm Log** from the **Monitor** menu. The Alarm Log lists all alarms that have occurred since the last time OpenView was restarted. You can display either **Current** (unacknowledged) alarms or **History** (acknowledged) alarms.

You can resize the columns in the Alarm log window by dragging the "I" character in the column labels with the mouse.



CH15-30

You can list the alarms either by the order received or severity using the **Sort by** controls in **Customize Alarms** in the **Options** menu.



CH15-37

Select **Time** as the sort criteria if you want the alarms to be listed in chronological order with the most recent alarm at the top of the list.

Select **Status** as the sort criteria if you want the alarms to be listed by the severity of the alarms. Critical alarms are grouped before warning alarms, and alarms within status groups are displayed in chronological order.

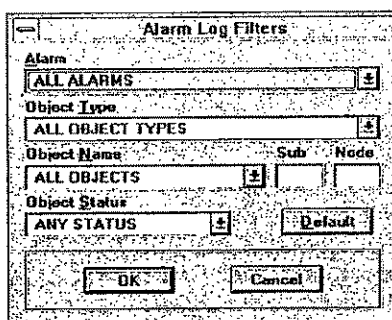
The Alarm Log can display up to 900 alarms. Refer to the next section *Selecting Alarms for Display* for instructions on how to select the alarms displayed.

Selecting Alarms for Display

You can display selected groups of alarms from the alarm log. Alarm displays can be limited to a type of device, specific device, or class of alarm severity. To configure an alarm display, click on **Filters** in the **Alarm Log** window. This will display the **Alarm Log Filters** dialog box.

The **Alarm Log Filters** dialog box contains the following entries:

- Alarm type (specific alarm name)
- Object Type (e.g. Personal Computer)
- Object Name (e.g. PC #21)
- Object Status (e.g. Critical)



Alarm type – This field allows you to select the alarm message type to be displayed. If you have several OpenView applications, each has its own set of alarms and associated messages. Refer to your application documentation for additional information. To select an alarm type, display the alarm type list and select one or all alarm types from the list. The default is **All Alarms**.

Object Type – This field allows you to select the types of devices (e.g., hubs, PCs, etc.), whose alarms you want to display. To select an object type, display the list of object types and select one or all object types. The default is **All Object Types**.

Object Name – This field allows you to select individual devices (e.g., hub #1, PC # 3, etc.) whose alarms you want to display. To select object names, display the list of object names and select one or all names. The default is **All Objects**.

In addition to specifying map objects by their names, you can also report on specific sub components in a device. To do this enter the desired **Subcomponent** or **Node** numbers for the subcomponent devices.

Object Status – This field allows you to select the types of alarms you want to display. To select status type, display the list of status types and select one or all status types. The default is **Any Status**.

Acknowledging and Deleting Alarms

To acknowledge or "clear" an alarm, select the alarm in the current list, and click **Acknowledge**. (Note that this does not delete the alarm entry. It moves the entry from the current to the history portion of the alarm log.) The color of the Alarm button on the tool bar is updated to the status of the most severe alarm remaining. The **Acknowledge** button is disabled unless an alarm is selected. When the last alarm in the list is acknowledged, the **Acknowledge** button is grayed to indicate that there are no more unacknowledged alarms. You can select multiple alarms to be cleared using **Ctrl** - click.

To acknowledge all alarms in the list, click **Acknowledge All**.

To delete all of the alarms from the history log, click on **Delete All**. To delete selected alarms from the history log, click on **Delete**.

To display a submap showing the device that generated an alarm, select the alarm in the list, then click **GoTo**. If possible, the device will be shown in the middle of the map window. If there are multiple instances of the device in the map, a dialog box is displayed to allow you to select the desired submap. If the multiple instances are on different submaps a dialog box will be displayed asking you which submap you wish to use to view the device. If the device does not exist in the map,

an error message is displayed. The GoTo button is disabled unless an alarm is selected.

If there is additional information about a selected alarm the **More Info** button will be enabled. To display the additional information, click on it to view the additional information in a separate dialog box.

- To close the Alarm Log window, click **Close**.

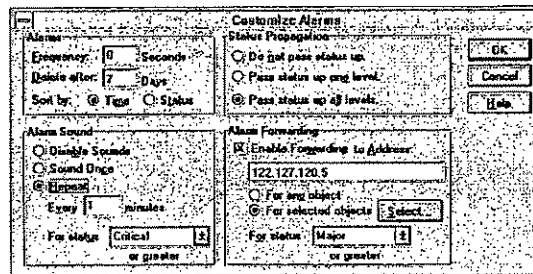
The alarm log can hold a large number of alarms and is limited primarily by the amount of disk space available. The number of entries in the log that can be displayed is limited by the amount of RAM memory available. You can configure OpenView to delete acknowledged alarms after a set number of days using **Customize Alarms** in the **Options** menu. Normally this will be sufficient to maintain a manageable log. If it is necessary to save the alarm data beyond the configured date, you can copy the contents of the alarm database files to archive files.

Configuring Alarm Processing

You can control the way OpenView processes alarm information. The major configuration groups for alarms are:

- Alarms (general)
- Alarm.Sound
- Status Propagation
- Alarm Forwarding

To set the alarm options, choose **Customize Alarms** from the **Options** menu to display the following dialog box:



General Alarm Settings

The general alarm settings include:

- The frequency at which multiple alarms are recognized
- The length of time that acknowledged alarms are stored in the Alarm Log
- Whether alarms are displayed by time or status level in the Alarm Log window.

Frequency – This setting is used to prevent multiple alarms of the same state from the same device. Duplicate alarms will be ignored if they occur within the specified time period. The default time is 0 seconds. A duplicate alarm occurring after this time will generate a new entry in the alarm log.

Delete After – This field is used to delete acknowledged alarms from the alarm database after the specified number of days. When OpenView is started and at midnight (if OpenView is running) any acknowledged alarms exceeding this time will be deleted from the database.

Sort By – This field selects whether the alarm log displays alarms in order received (most recent first) or by order of severity, i.e. most critical alarms first. Alarms of the same severity are ordered by time. Note that the color of the Alarm button in the toolbar and the color of an iconized Alarm Log or submap will show the status of the most severe unacknowledged alarm regardless of the **Sort By** setting.

Alarm Sound Settings

Alarm Sound – The settings control the sounds generated by an alarm. Note that no sound will be generated regardless of the setting unless the application managing a particular device requests an audible alarm. The alarm sound settings allow you to control:

- whether sounds are enabled
- whether a sound alarm is generated only once
- if an alarm is to be repeated, the repeat rate for each status of alarm



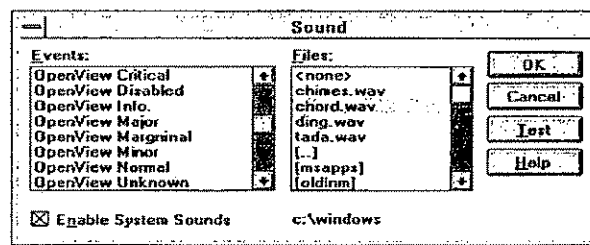
You must also have an appropriate sound driver program installed.

Disable Sounds – This turns off sound for all alarms, **Sound Once** will play the appropriate alarm sound when the alarm is generated. The

Repeat setting will play reminder sound every **x** minutes until the alarm is acknowledged. The sound used for the **Repeat** setting will be that for the most severe uncleared alarm at or above the selected status level. For the example shown, a sound is generated whenever an alarm is generated and a sound will be generated every minute if there are any unacknowledged Major or Critical alarms.

Alarm Sound Configuration

OpenView can generate a sound when a device changes status, and a different sound can be generated for each status level. If you have a sound card and drivers installed, you can use the **Sound** dialog in the Windows Control Panel to associate OpenView alarms with any Windows .wav wave file. Otherwise, the system beep will be used for all alarm sounds.



CH5-49

Alarm Status Propagation

The **Status Propagation** field controls how alarms are passed between submap levels. The **Status Propagation** setting allows you to select from one of following three status propagation methods:

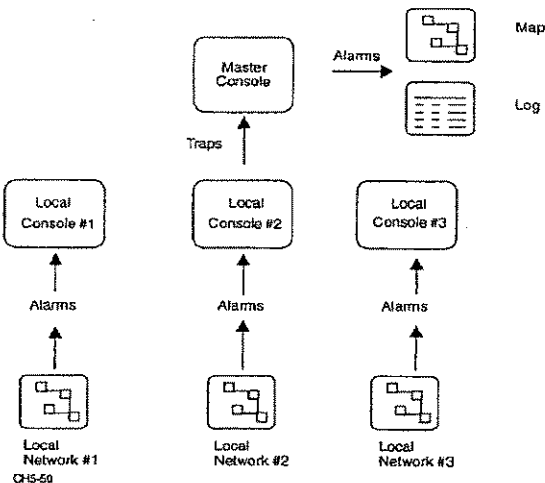
- do not propagate status
- propagate status to the next higher submap only
- propagate status to all higher submaps

If status is not passed up, submap symbols at higher levels remain unchanged when devices under them change status. If status passes up one level, the submap symbols are displayed with the color of the most severe status of all devices on the level below them. If status passes up all levels, submap symbols are displayed with the color of the most severe status of all devices contained on any level below them. When a submap is minimized, its icon will be the color of the most severe status

contained in the submap and will propagate status based on the Status Propagation configuration.

Alarm Forwarding

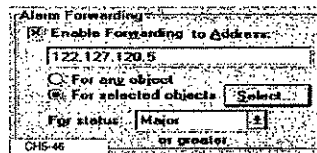
Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console.



To forward alarms you must configure the following:

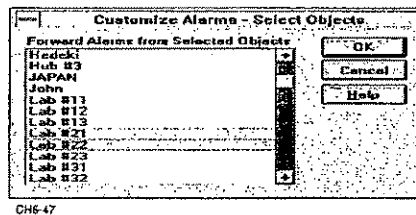
- The address of the console to receive the trap
- The map objects whose alarms are to be forwarded
- The types of alarms to be forwarded

The alarm forwarding is configured using the **Alarm Forwarding** box of the **Customize Alarms** dialog box.



- 1 Enter the address of the console where the forwarded alarms are to be sent.
- 2 Select the map objects whose status is to be forwarded.

If you do not want alarms for all objects on your map to be forwarded, click on the Select button. This will cause a list of map objects to be displayed. You can then select the desired objects.



- 3 Select the status levels that are to be forwarded.
- 4 Click on OK in the main Customize Alarms dialog box.

This will save your alarm forwarding information in the OVWIN.INI file.

In the example shown above, two devices, Lab #21 and Lab #22 will forward alarms of Major or Critical status to an OpenView console at address 122.127.120.5.

Running Programs

OpenView can run an MS-DOS or Windows program when an alarm is generated. You can select what program is run based on the status of the alarm. Information about the alarm can be passed as command line arguments to the program. You control the program trigger function by making entries in the owin.ini file before running OpenView.

(Note that if the alarm is generated by an application program, the application program must have enabled programs to be run in response to the alarm. Refer to documentation for the application program responsible for generating the alarm. Program execution is enabled for

4-30

CHAPTER 4: MONITORING DEVICES ON THE NETWORK

alarms generated by the polling and trap management features of OpenView.)

To run a program for a particular level of alarm, add an entry to the [OVAAlarm] section of ovwin.ini as follows:

```
RunCritical=<command line>
RunMajor=<command line>
RunMinor=<command line>
RunWarning=<command line>
RunMarginal=<command line>
RunNormal=<command line>
RunDisabled=<command line>
RunUnknown=<command line>
RunInformational=<command line>
RunUnmanaged=<command line>
```

where *<command line>* is the program name and parameters.

For example: RunCritical=write.exe readme.wri will run MS Write and display the file readme.wri.

OpenView provides alarm information in the following command line variables:

%a	Alarm text	%o	Object name
%i	Alarm type ID	%p	Alarm application ID
%m	More info field	%s	Subobject number
%n	Node number	%t	Time of alarm
		%y	Object type

The command line can include these variables to provide more information about the alarm.

For example, if the entry in the OVWIN.INI file for RunCritical was:

```
RunCritical=prog.exe %t - %o - %a
```

then a **critical** alarm on **Brian's PC** at **2:30** on **Feb 16** would execute the following:

```
prog.exe Tue Feb 16 14:30:05 1993 - Brian's PC - Power Supply
Overheating
```

DDE Commands In addition to running a program with a command line string, the alarm system can also pass information to another Windows application using DDE. Refer to Microsoft Windows documentation for more information on DDE operation. DDE exchanges are indicated using the ">" character after the "=" sign in the Run entry in the *ovwin.ini* file. DDE Run commands use the following format:

```
RunCritical => <program>,<service>,<topic>;<command>
```

When an alarm occurs, OpenView will attempt to establish a DDE conversation with the specified **service** and **topic**. If the connection to the service cannot be established, the indicated **program** will be run and another attempt made to establish the conversation. Once established, OpenView will send a DDE Execute message of **command**, and will then terminate the conversation.

Paging Program OpenView ships with the paging program *Notify! Connect* from Ex Machina Corporation. This program sends a paging message to a pager when a specified alarm goes off.

For example, *Notify! Connect* supports the DDE NOTIFYservice and SendPage topic. It sends a pager message when sent a command of the form **Username, Message**. The *ovwin.ini* entry would be as follows:

```
RunCritical => c:\ov\notify\connect.exe,NOTIFY,SendPage;OpenView,Critical Alarm: %o - %a
```

This will send the following pager message to OpenView when a critical alarm occurs:

```
Critical Alarm: Brian's PC - Power Supply Overheating
```

For more information about *Notify! Connect*, refer to the *Notify! Connect* documentation.

Alarm Database Every alarm is recorded in an alarm database. Each entry contains the date and time, status, device name, and device type of the alarm.

The alarm log is saved in Borland Paradox database format. The files are named *ovalins.** and are stored in the OpenView directory (OV). You

can copy these files for archival purposes and save alarm history information beyond the deletion date. You can also use a Paradox database application to access the database and create reports or manipulate the archived files.



CAUTION: Do not make changes directly to the OVALINS.* files as this can cause improper operation of OpenView.

The database uses one record for each alarm with a primary key on time and a secondary key on status. The record structure is as follows:

Table 4-3 Database Records

Field	Format	Description
key	number	Paradox database key, combination of time and object ID.
date	date	Date at which the alarm occurred.
hours	time	Hour at which the alarm occurred.
minutes	time	Minute at which the alarm occurred.
seconds	time	Second at which the alarm occurred.
severity	number	Severity of alarm, Critical=10, ..., Unmanaged=1.
application ID	number	Application that generated the alarm.
device class	number	Device class.
not used	-	-
open/cleared	number	Alarm state, Open=0, Cleared=1.
device type	number	Device symbol number.
device name	64 characters	Name of the map object that generated the alarm.
subcomponent	number	Subcomponent number or -1 if not used.
node	number	Part number of subcomponent or -1 if not used.
status	number	Current status.
message	64 characters	Alarm text displayed for this alarm.
extended description	blob text	Extended description of a field, activated by the More Info button.

DMI Manager

The DMI Manager in the Control Menu allows you to query DMI capable PCs to determine their capabilities, configuration, and status. The interface and dialogs for the DMI Manager are very similar to those of the SNMP Manager. The variables that can be accessed are defined by the DMTF (Desktop Management Task Force). You do not need to compile sets of variables for each device type. A given device type may not support all of the DMI variables. Additional information on the DMI Manager is given in the online help.

DMI Manager **4-33**

HP Top Tools HP TopTools is a management tool for DMI (Desktop Management Interface) capable PC's on your network. Select DMI PC objects on the map to retrieve system and tattoo information about the PC and remotely configure BIOS parameters and security features on the selected PC. For more information, run HP Top Tools and refer to the online help. (Refer to the DMI Manager in the Control Menu for additional information.)

4-34 CHAPTER 4: MONITORING DEVICES ON THE NETWORK

SYM_P_0081032

5

MANAGING SNMP NETWORK DEVICES

The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB). A MIB contains variables that describe the characteristics and current state of a network device. The SNMP Manager can access this information and control network devices that support SNMP.

You can manage an SNMP device by querying or setting its MIB variables. The SNMP Manager supports all Internet MIB-II variables and can be extended to support other MIBs. Operations on MIB-II variables, such as **egp** and **transmission**, will not return values from devices supporting only MIB-I.



In order to manage or query an SNMP device, you must log in as a supervisor or operator.

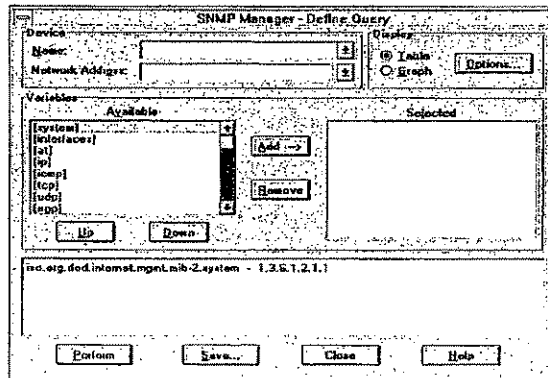
This chapter provides information about how to define, select and display the query results as a table or graph. It also tells you how to manage the SNMP database.

The OpenView SNMP Manager uses information from MIB files provided by network device manufacturers to build its own database. This database tells the SNMP Manager what device variables are available to query. If you are not familiar with MIBs you should read the section *Managing the SNMP Manager Database* later in this chapter.

Defining a Query

OpenView allows you to generate tables or graphs about information available in a device's MIB database. To define a query, you select a device and then select the variables that you want to query.

To define a query, choose **Define Query** from **SNMP Manager** in the **Control** menu. The following dialog box appears:



To select a device to query you must supply the network address. If an object is selected on the map, its device name and network address will appear in the Device fields.

To select a device to query, use one of the following procedures:

- Select a device from your map before you open the SNMP Manager.
- Click on the **Name** field or use the list button to view the list of all devices configured in your current map. You can then scroll through the list to select the desired device. (If the list of devices is long, some may not be displayed. You will then need to select the device from the map or type in the network address.)
- Type the first letter of the device name in the name field. The device list from the current map automatically appears and jumps to the first entry starting with that letter. Pressing that letter repeatedly scrolls through the list of all devices starting with that letter.

Once the device name is selected, the network address, as configured for the device in your map, appears in the Network Address field. If no address was configured in the map, type the network address into the field. The SNMP Manager uses the network address, not the device name, to perform the actual query.

You can also select a device when you only have the network address. You can use this method to access a device that is not part of your current map:

- Type in the network address in the **Network Address** field. The network address does not have to be associated with the current map. The device name will be blank. Addresses must be in IP format (123.123.123.123) or IPX format (12345678-123456789012).

Device

Name:

Network Address:

CH6-04

Selecting Variables to Query

The accessible SNMP variables are listed in the Variables box and may come from various MIBs. An extensive set comes with OpenView. Applications installed into OpenView may have added their own MIBs to the list. You may also use the MIB compiler to add MIBs.

The variables are displayed in a tree fashion with the MIB-II level displayed as a default. The following map will help you navigate through the tree. Additional information about the map and compiling MIBs can be found in the MIB Maps section of this chapter.

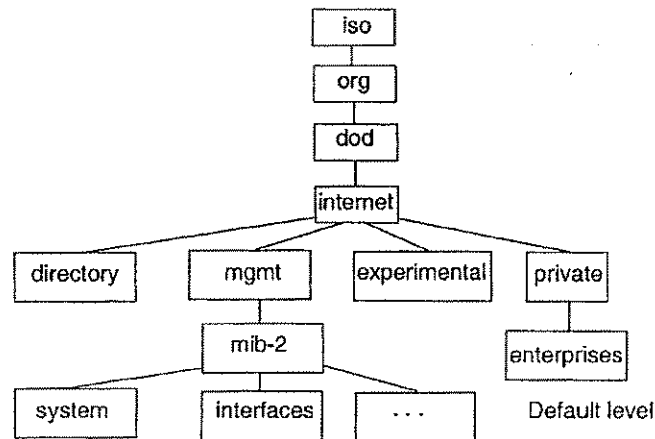
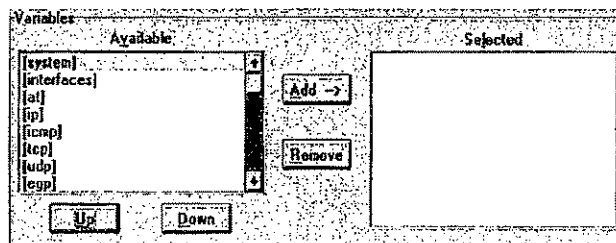


Figure 5-1 MIB variables tree

Moving Around the Variable Tree

To move around the variable tree, follow these steps:

- 1 Select the group variable you want to query.
For example, select [system].
- 2 To move up the tree, click on Up (this would move you to mib-2).
- 3 To move down the tree, click on Down (or double-click on the variable name).



CH6-65

Entries in the variables list are displayed using the following format:

Table 5-1 Variables List

Format	Description
{square brackets}	denote a group that contains additional variables
{curly braces}	denote SNMP tables
"double quotes"	denote textual values

If you select a group variable to query, all variables in that group will be part of that query. Queries can be for a single table variable (for example, **{atTable}**) several values from a given table, or one or more non-table variables (**ipInReceives**). If an SNMP table variable is selected, no other variable may be selected.

Individual values (columns) may be selected for an SNMP table by clicking on the **Down** button to move down the tree below the table and entry definitions to the individual column variables. You may select multiple column table variables and then click on **Add** to add these to the query. In this case, any previously selected variables are removed from the selection list, as only columns within a single table may be queried.

Selecting a Variable to Use in the Query

To select a variable to use in the query, follow these steps:

- 1 In the Available variables box, click on a single variable you want, or ctrl-click to highlight more than one variable.
- 2 Click Add.

The variable name will move into the Selected Variables box.

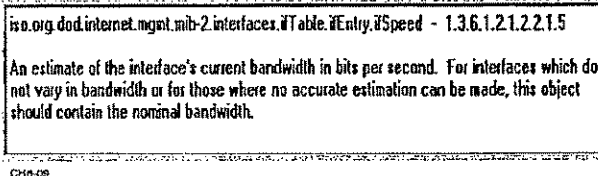
Removing a Variable From the Query List

To remove a variable from the query list, follow these steps:

- 1 In the Selected variables box, highlight the variable you want to remove.
- 2 Click Remove.

It disappears from the Selected Variables box.

Variable Descriptions When you highlight a variable, the corresponding description is displayed in the Description box. For example, the description for ifSpeed ([interfaces.], {if Table},{ifEntry}) would be as shown.



The Description box displays information about the variable highlighted in the Available or Selected variables boxes. This information uses the standard format for SNMP object identifiers (OID 1.2.3) and an associated description.

Saving a Query

You can save a query so that you can query a selected device in the future or use it as a template for creating other queries.

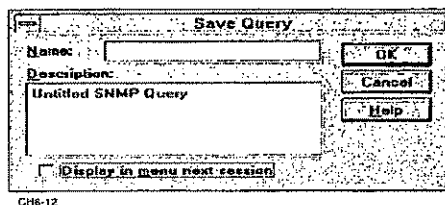
To save a query, follow these steps:

- 1 Make sure all of the information you want to save has been entered into the Define Query window.

You should perform the query to make sure it generates the expected report.

- 2 Click on Save.

The following window is displayed.



- 3 In the Name field, type in a filename of up to 8 characters.

Selecting a Query 5-7

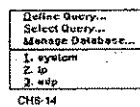
Do not enter a file extension – OpenView will append the .OVQ file extension when the file is saved.

- 4 If you want, you may use the Description field to describe the saved query.

This is especially helpful where the query has a specific use in your environment or where the query is to be used by others.

- 5 Make your choice in the check box.

If this box is checked, the next time you start OpenView, the query is listed in the menu under the SNMP Manager command. There is no limit to the number of queries that can be saved.



- 6 Click OK.

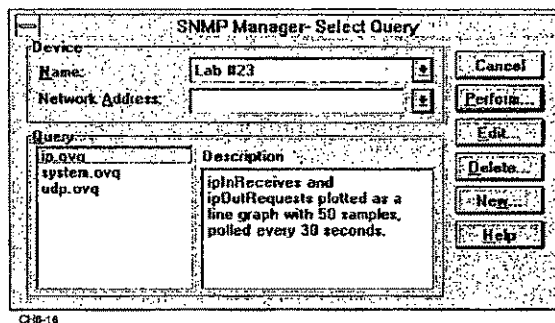
To perform, edit, or delete saved queries, choose **Select Query** from **SNMP Manager** in the **Control** menu. The queries are stored as separate files with the .OVQ extension in the OpenView directory.

Selecting a Query

Selecting a query allows you to perform, edit, or delete the query.

To select a query, follow these steps:

- 1 Choose Select Query from SNMP Manager in the Control menu.
The following dialog box appears.



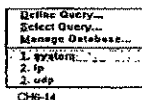
2. Highlight a saved query from the list in the Query box.
A description of the query appears in the Description box.
3. If you want, change the device name and address in the Device box.
4. Click on the appropriate function listed below for the action you want:

Table 5-2 Select Query Functions

Button	Description
Perform	Executes the Query.
Edit	Opens the Define Query window and inserts the query selected in Select Query. Modifications can be made and saved under the same or a new name.
Delete	Deletes the query file and all references to the query.
New	Opens a blank Define Query window.

Removing a Query from the Menu

Since there is a limit of nine queries that are listed in the menu, you may want to remove a query from the menu commands.

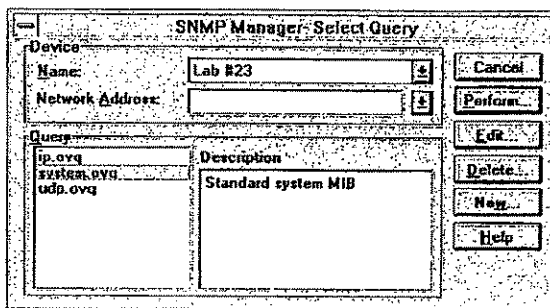


Removing the query from the menu does not delete the query. To delete the query, select the query and click on **Delete** in the Select Query dialog box. See the previous section, *Selecting a Query for information*.

Displaying SNMP Query Results **5-9**

To remove a query from the menu, follow these steps:

- 1 In the Select Query dialog box, select a query in the query box.



CH5-17

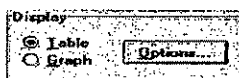
- 2 Click on Edit.
The Define Query window is displayed.
- 3 Click on Save.
The Save Query window is displayed.
- 4 Remove the x in *Display in menu next session* by clicking on the check box.
- 5 Click on OK.
- 6 Close the Define Query window.

The menu change takes effect when you restart OpenView. (Exit OpenView and restart.)

Displaying SNMP Query Results

After you select the devices and variables you want to query, you can display the query results as a table or a graph. This section describes how to display query results as a table.

To choose the table or graph display option, select **Define Query** from **SNMP Manager** in the **Control** menu.



CH5-18

Displaying a Query as a Table

Table queries can be for a single table variable (a table variable is displayed in {curly braces} in the variable list), for one or more non-table variables.

The format of the table generated varies, as follows:

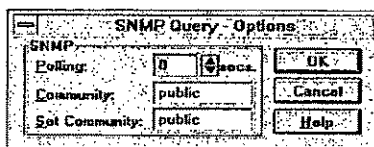
- If the query contains an SNMP table, the variable names will be displayed across the top of the table. There will be numbered rows below the heading. You can scroll through the rows, but cannot add or delete rows.
- If the query does not contain an SNMP table, the values are listed in scalar format. Any group that you request in the query will be expanded to list individual variables.

Values within a table may appear as strings, integers, network addresses, or object names displayed in 1.2.3 notation. Other data, such as a MAC address, will appear in hexadecimal format (for example: 01 F3 07).



OpenView supports a maximum of 999 rows in each table. If your computer doesn't have enough memory, the table may not be able to reach this limit. To minimize network traffic and memory requirements, select only the columns that you want to display. For information about how to select specific columns, see the example under Performing a Query.

After selecting to display your query results as a table, click on **Options** in the Display section of the **Define Query** dialog or **Table** dialog box. Then set the polling interval and enter the Community and Set Community names.



CH5-19

Figure 5-2 Table format query options dialog